IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Abraham R. MATTHEWS	**Examiner:** SHIN, Kyung H.
App. Control No.: 09/661,637	Technology Center (TC): 2100
Filed: September 13, 2000	Group Art Unit: 2143
For: SYSTEM AND METHOD FOR DELIVERING SECURITY SERVICES	Conf. No.: 7670
	Docket No.: FORT-000100

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Applicant (hereafter "**Appellant**") hereby submits this Brief in support of its appeal from a decision by the Examiner, mailed September 11, 2007, in the above-captioned application. Appellant respectfully requests consideration of this Appeal by the Board of Patent Appeals and Interferences (the "**Board**") for allowance of the above-captioned patent application.

On February 11, 2008, the Appellant submitted a Notice of Appeal (via EFS Web) in the above-captioned patent application concurrently with a Response Under 37 C.F.R. §1.116. The claims of the above-captioned patent application were finally rejected by the Examiner in a final Office Action mailed September 11, 2007 (the "**Final Office Action**"). Therefore, this is a proper Appeal and Appellant's Brief in support of this Appeal follows.

TABLE OF CONTENTS

Table of Contents 2
Real Party in Interest 3
Related Appeals and Interferences 4
Status of Claims 5
Status of Amendments 6
Summary of Claimed Subject Matter 7
Claims Appendix 17
Evidence Appendix 20
Related Proceedings Appendix 21

REAL PARTY IN INTEREST

The real party in interest in this Appeal is Fortinet, Inc., the assignee of record of the above-referenced patent application.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences related to this Appeal.

STATUS OF CLAIMS

Claims 19-27 are currently pending in the above-captioned patent application. In the Final Office Action, the Examiner (1) rejected claims 19-24, 26 and 27 under 35 U.S.C. §103(a) as allegedly being unpatentable over US Patent No. 6,466,976 of Alles et al. (hereafter "**Alles**") in view of US Patent No. 6,453,406 of Sarnikowski et al. (hereafter "**Sarnikowski**") and further in view of US Patent No. 6,674,756 of Rao (hereafter "**Rao**"); and (2) rejected claim 25 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Alles, Sarnikowski and Rao and further in view of US Patent No. 6,243,580 of Garner (hereafter "**Garner**").

Claims 19-27 as set forth in the Amendment and Response to Office Action submitted June 20, 2007, are the subject of this Appeal. The Claims Appendix below sets forth a copy of the appealed claims.

STATUS OF AMENDMENTS

After the Final Office Action, which finally rejected claims 1-27, the Appellant, in an effort to reduce issues on appeal, submitted a Response under 37 C.F.R. §1.116 on February 11, 2007 (the "**Amendment After Final**") amending the specification of the above-captioned patent application and cancelling claims 1-18. The amendments proposed in Amendment After Final have been acted upon by the Examiner. The Advisory Action mailed on March 4, 2008 (the "**Advisory Action**") indicates for purposes of appeal, the proposed amendments would be entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The sole remaining independent claim in the above-captioned patent application, i.e., claim 19, generally relates to a method of delivering security services, such as Virtual Private Networks (VPNs) and managed firewall services, to multiple subscribers of a service provider[1]. Processors[2] of a first service processing switch[3] at a first point-of-presence (POP)[4] associated with a first site of a first subscriber[5] and a first site of a second subscriber[6] and processors[7] of a second service processing switch[8] at a second POP[9] associated with a second site of the first subscriber[10] and a second site of the second subscriber[11] are logically connected into packet-passing ring configurations[12]. A set of virtual routers[13] is established on the processors of each of the service processing switches. The subscribers are each provided with their own set of customized application layer services and the resources allocated to each subscriber are appropriately isolated by: partitioning the virtual routers between the subscribers and providing the subscribers with virtual private networks (VPNs)[14] communicatively coupling their respective sites. A first partition of the virtual routers is initially allocated and configured for use by the first subscriber and a second partition of the virtual routers is initially allocated and

---

[1] See, e.g., specification p. 8, ll. 18-23 and FIG. 4.
[2] See, e.g., 930 or 935 of FIG. 9 discussed at specification, p. 16, ll. 6-14.
[3] See, e.g., 201-1 of FIG. 4 discussed at specification, p. 12, ll. 19-24.
[4] See, e.g., 201 of FIG. 13 discussed at specification, pp. 28-33 with reference to exemplary network-based model "Architecture Four."
[5] See, e.g., 412 of FIG. 4 discussed at specification, p. 12, ll. 4-6.
[6] See, e.g., 422 of FIG. 4.
[7] See, e.g., 930 or 935 of FIG. 9 discussed at specification, p. 16, ll. 6-14.
[8] See, e.g., 201-2 of FIG. 4 discussed at specification, p. 12, ll. 24-28.
[9] See, e.g., 201 of FIG. 13 discussed at specification, pp. 28-33 with reference to exemplary network based model "Architecture Four."
[10] See, e.g., 411 of FIG. 4 discussed at specification, p. 12, ll. 4-6.
[11] See, e.g., 421 of FIG. 4.
[12] See, e.g., counter-rotating dual ring 232 of FIG. 2 and FIG. 5 discussed at specification, p.10, ll. 23-27 and specification, p. 13, ll. 22-23; and packet-passing data rings 933 and 934 of FIG. 9 discussed at specification, p. 16, ll. 7-8 and ll. 22-25 as well as specification, p. 17, ll. 5-8.
[13] See, e.g., set of partitioned virtual routers 210 of FIG. 4 discussed at specification, p.12, l. 4 to pg. 13, l. 2.

configured for use by the second subscriber; however, depending upon the relative processing demands of the respective customized application layer services, processing capacity can be dynamically shifted as needed by reallocating resources of either the first service processing switch or the second service processing switch between the partitions of virtual routers[15]. As discussed at Specification, pp. 19-36, managed, network-based security services implemented in the manner claimed provide advantages in terms of at least cost-efficiency, flexibility, manageability, scalability and complexity over customer-premises equipment (CPE)-based systems.

[14] See, e.g., 410 and 420 of FIG. 4 discussed at specification, p. 12, ll. 1-6 and ll. 11-17.
[15] See, e.g., Specification, p. 6, ll. 13-15; Specification, p. 12, ll. 9-14; Specification p. 12, ll. 14-17; Specification, p. 12, ll. 18-19; and original claims 16 and 18.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Did the Examiner improperly reject claims 19-27 under 35 U.S.C. §103(a) by attributing capabilities and functionality to the combination of references relied upon that are clearly unsupported by and outside of the scope and contemplation of such references?

ARGUMENT

A. The Examiner improperly rejected claims 19-27 under 35 U.S.C. §103(a) by attributing to the combination of references relied upon capabilities and functionality that are neither required, taught, nor reasonably suggested by their combined disclosures.

Claims 19-27

In the Final Office Action, the Examiner incorrectly rejected claims 19-24, 26 and 27 under 35 U.S.C. §103(a) as being unpatentable over Alles in view of Sarnikowski and further in view of Rao. It is respectfully submitted that the Examiner has failed to establish a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness, the prior art references when combined must teach or suggest all the claim limitations (MPEP 706.02(k)). In the present case, none of the cited references teach or reasonably suggest at least the expressly recited element of "***providing changeable provisioning of processing capacity*** between the first subscriber and the second subscriber ***by programmatically dynamically reallocating resources*** of the first service processing switch or the second service processing switch ***between the first partition and the second partition*** based on comparative processing demands of the first set of customized application layer services and the second set of customized application layer services" (emphasis added, hereafter the "**Element At Issue**").

In the Advisory Action, the Examiner indicated:

> The reallocation of resources is not dynamic or programmatically based in the specification.
>
> According to Application Spec [pg 12 ll 14-17; SMS 221 running on SP network 200 allows ease of service provisioning (dynamically adding additional processors/processing power when needed, reducing the processors/processing power used for VPN 410 when not needed).], an increase or decrease in the number of processors impacts processing provisioning.
>
> Alles (6,466,976) discloses changeable provisioning by changing the number of processors;
>
> [col 3, ll 36-41; The physical separation enables the number of processors and ports to be changed (increased or decreased) independent of each other. The resulting flexibility enables an architecture in accordance with the present invention to scale well to support a large number of subscribers.], and a change in processing
>
> [col 4, ll 3-8; The present invention enables an ISN to scale well to serve a large number of subscribers as the number of processors can be increased and the computation load of processing packets can be distributed among the processors.

With respect to the Examiner's statement that "[t]he reallocation of resources is not dynamic or programmatically [*sic*] based in [*sic*] the specification," the undersigned believes this apparent new written description rejection under 35 U.S.C. §112, 1st paragraph should have been raised in the Final Office Action to be considered as part of this Appeal; however, for completeness, the undersigned will address this new rejection. In the context of a running computer system, the term "dynamic" generally refers to an operation that occurs at the time it is needed rather than at a predetermined or fixed time. The term "programmatic" generally refers to resembling, or having a program or following a plan, policy, or program. The undersigned respectfully submits the Specification makes it clear that the reallocation of processing and/or storage resources among customers can be performed both dynamically and programmatically. For example, see Specification, p. 6, ll. 13-15 ("[t]his solution can be changes [*sic*: changed] to ***provision each customer with more or less processing power and storage, according to individual changing needs***."); Specification, p. 12, ll. 9-14 ("[s]ince each VR 410 is supported by an object group 211, ***objects can be easily added or omitted to enable customized services on a subscriber-by-subscriber basis*** to meet each subscribers individual needs."); Specification p. 12, ll. 14-17 ("SMS 221 running on SP network 200 allows ease of service provisioning (***dynamically adding additional processors/processing power when needed, reducing the***

processors/processing power used for VPN 410 ***when not needed***)."); Specification, p. 12, ll. 18-19 ("[i]n some embodiments, IPNOS 223 uses an open ***Application Program Interface (API) to enable new services to be added to the platform whenever needed***.") (Emphasis Added). In view of at least the foregoing, it should be clear that the Specification provides adequate support for reallocation of virtual router resources, such as processing power and storage, among subscribers "dynamically" (e.g., on an as-needed-basis as opposed to on a fixed or static schedule). Additionally, it should be clear that the Specification provides adequate support for such reallocation to be performed "programmatically" (e.g., in accordance with a plan, policy, or program) as defined by programming instructions associated with an open Application Program Interface (API), for example.

Turning now to the obviousness rejection, this rejection also appears to have been revised by the Examiner in the Advisory Action. For completeness, the undersigned will address both the original rejection of claim 19 as set forth in the Final Office Action as well as the newly added rejection in the Advisory Action.

In the Final Office Action at pp. 13-14, the Examiner indicated:

> **Regarding Claim 19**, Alles discloses a method comprising:
>
> [...]
>
> j) providing changeable provisioning of processing capacity between the first subscriber and the second subscriber by programmatically dynamically reallocating resources of the first service processing switch or the second service processing switch between the first partition and the second partition based on comparative processing demands of the first set of customized application layer services and the second set of customized application layer services. (see Alles col. 8, lines 4-9; col. 8, lines 11-15; col. 8, lines 48-52: reallocate resources between subscribers, dynamically)

As can be seen from the above-cited portion of the Final Office Action, the Examiner initially indicated the Element At Issue was disclosed by Alles at "col. 8, lines 4-9; col. 8, lines 11-15; col. 8, lines 48-52." These portions of Alles are reproduced below for the Board's convenience.

Alles, col. 8, ll. 4-9:

> Conditions may be specific to the type of service policy being implemented. For example, a subscriber may be permitted higher bandwidth during non-business hours. Another subscriber may have the data being given a lower priority if the data is destined to a specific subscriber during a specified time of day. Examples of the conditions are

Alles, col. 8, ll. 11-15:

> Many processing rules may be generated up-front when the service policies are specified. However, for some processing rules, the necessary information may not be available up-front. In such a situation, rules are generated dynamically when the information is available. Some

Alles, col. 8, ll. 48-52:

> It may be noted that some of the processing rules may be instantiated up-front, for example, at the earlier of when ISN 150 boots up or when the desired services are specified. Some other processing rules may be instantiated when generated as described above in step 225.

As the undersigned attempted to explain in the Amendment After Final, ***the portions of Alles cited by the Examiner appear to relate to dynamic generation of processing rules***. While the above-cited portions of Alles contain one or more forms of the word "dynamic," it is respectfully submitted ***these portions of Alles do not relate to providing changeable provisioning of processing capacity between subscribers as a result of dynamic reallocation of resources between partitions of virtual routers*** as required by the Element At Issue. As the undersigned also attempted to explain to the Examiner in the Amendment After Final, the mere fact that Alles mentions a subscriber may be permitted higher bandwidth during certain times (as a result of application of the subscriber-specific processing rules) does not reasonably suggest

the dynamic reallocation of resources between partitions of virtual routers as required by the Element At Issue. Instead, ***this statement in Alles implies all resources are common resources available to all subscribers*** (rather than allocated and isolated as recited by claim 19) and application data flows are controlled by the subscriber-specific processing rules (possibly indirectly limiting access to the shared resources, but more likely used as a mechanism for prioritizing among application data flows). Alles' use of subscriber-specific processing rules is simply not comparable to reallocating resources between partitions of virtual routers as required by the Element At Issue. For at least these reasons, Alles clearly lacks the teaching and/or suggestion attributed to is by the Examiner and independent claim 19 is patentably distinguishable over Alles.

As indicated above, in the Advisory Action, the Examiner's obviousness rejection was restated and now apparently relies on col. 3, ll. 36-41 and col. 4, ll. 3-6 for the purported teaching regarding the Element At Issue. Again, for the Board's convenience, the undersigned has reproduced the relevant portions of Alles below.

Alles, col. 3, ll. 36-41:

> The processors processing the packets (to provide the desired services) may be provided as physical units separated from the access and trunk ports. The physical separation enables the number of processors and ports to be changed (increased or decreased) independent of each other. The resulting flexibility enables an architecture in accordance with the present invention to scale well to support a large number of subscribers.

Alles, col. 4, ll. 3-6:

> The present invention enables an ISN to scale well to serve a large number of subscribers as the number of processors can be increased and the computation load of processing packets can be distributed among the processors.

Importantly, neither of these portions of Alles, address the deficiencies noted above in relation to Alles' lack of teaching regarding "providing changeable provisioning of processing

capacity" between subscribers "by programmatically dynamically reallocating resources" among partitions of virtual routers. The first portion of Alles merely indicates the processors are physically separate from the access and trunk ports, thereby allowing the number of processors to be increased or decreased independent of the access and trunk ports. The second portion of Alles simply points out the computational load of packet processing may be distributed among the processors of the ISN 150 and confirms the undersigned's earlier suggestion that all processing resources of the ISN 150 are treated as a common pool of resources to be shared by the subscribers without any apparent mechanism to isolate one subscriber from another. Thus, Alles appears to allow the number of processors of the ISN 150 to be manually increased or decreased independent of the access and trunk ports; however, such manually changeable processing capacity is firstly not between subscribers; and secondly not as a result of programmatically dynamically reallocating resources between partitions of virtual routers.

Finally, none of Sarnikowski, Rao or Garner are relied upon by the Examiner for teaching or suggesting the Element At Issue and the undersigned has found nothing in the disclosures of Sarnikowski, Rao or Garner relating to providing changeable provisioning of processing capacity between subscribers by programmatically dynamically reallocating resources between partitions of virtual routers as required by the Element At Issue. For at least these reasons, independent claim 19 and its dependent claims, which add further limitations, are clearly distinguishable over the proposed combination relied upon by the Examiner.

As evidenced by the foregoing, the Examiner has incorrectly attributed teachings to Alles that are clearly absent from and not contemplated by the disclosure of Alles. The Examiner then proceeds to use such attributed teachings in combination with additional references to find

obviousness under 35 U.S.C. §103(a). For at least these reasons, the undersigned respectfully requests the Board to reverse the Examiner's obviousness rejections of claims 19-27.

CONCLUSION

The Examiner has failed to establish a *prima facie* case to support his 35 U.S.C. §103(a) rejections. The combination of Alles, Sarnikowski, Rao and Garner does not teach or reasonably suggest at least the Element At Issue of independent claim 19. The Examiner has improperly attributed teachings and/or functionality to Alles that are unsupported by, inconsistent with, not enabled by and outside the scope of the written description of Alles. For the aforementioned reasons, the Examiner's rejections should be reversed, and claims 19-27 should be allowed.

Respectfully submitted,
HAMILTON, DESANCTIS & CHA

Date May 8, 2008

By: /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 64128
Ph: (303) 856-7155

CLAIMS APPENDIX

19. A method comprising:

providing a first service processing switch at a first point-of-presence (POP) associated with a first site of a first subscriber of a service provider and a first site of a second subscriber of the service provider;

providing a second service processing switch at a second POP associated with a second site of the first subscriber and a second site of the second subscriber, wherein the first service processing switch and the second service processing switch are communicatively coupled via a network;

logically connecting a plurality of processors of the first service processing switch into a packet-passing ring configuration;

logically connecting a plurality of processors of the second service processing switch into a packet-passing ring configuration;

establishing a first set of virtual routers on the plurality of processors of the first service processing switch;

establishing a second set of virtual routers on the plurality of processors of the second service processing switch;

providing the first subscriber with a first set of customized application layer services and the second subscriber with a second set of customized application layer services and providing subscriber resource isolation by

partitioning the first set of virtual routers and the second set of virtual routers between the first subscriber and the second subscriber including (i) allocating and configuring a first partition, comprising a first subset of the first set of virtual routers and a first subset of the second set of virtual routers, to the first

subscriber and (ii) allocating and configuring a second partition, comprising a second subset of the first set of virtual routers and a second subset of the second set of virtual routers, to the second subscriber,

providing the first subscriber with a first virtual private network (VPN) communicatively coupling the first site of the first subscriber with the second site of the first subscriber by establishing a first secure tunnel through the network between virtual routers of the first partition, and

providing the second subscriber with a second virtual private network (VPN) communicatively coupling the first site of the second subscriber with the second site of the second subscriber by establishing a second secure tunnel through the network between virtual routers of the second partition; and

providing changeable provisioning of processing capacity between the first subscriber and the second subscriber by programmatically dynamically reallocating resources of the first service processing switch or the second service processing switch between the first partition and the second partition based on comparative processing demands of the first set of customized application layer services and the second set of customized application layer services.

20. The method of claim 19, wherein the first set of customized application layer services comprises firewall protection.

21. The method of claim 20, wherein the first set of customized application layer services comprises web site hosting.

22. The method of claim 20, wherein the first set of customized application layer services comprises e-mail services.

23. The method of claim 19, wherein the first secure tunnel and the second secure tunnel are established by sharing a single secure tunnel between the first service processing switch and the second service processing switch.

24. The method of claim 19, wherein in said providing changeable provisioning of processing capacity between the first subscriber and the second subscriber is controlled by a services management system of the service provider.

25. The method of claim 19, wherein the plurality of processors of the first service processing switch are associated with one or more control blades, one or more access blades, and one or more processing blades.

26. The method of claim 19, wherein packets exchanged between the first service processing switch and the second processing switch contain processor identifiers (PEIDs) that identify a processor of the plurality of processors of the first service processing switch or a processor of the plurality of processors of the second service processing switch to which the packets are destined.

27. The method of claim 26, wherein the packets contain logical queue identifiers (LQIDs) that identify a software entity to which the packets are destined within the identified processor.

EVIDENCE APPENDIX

NONE.

RELATED PROCEEDINGS APPENDIX

NONE.